REMARKS

Claims 1, 10, and 26-28 are pending.
Claims 1, 10, and 26-28 are rejected.

The office action dated November 10, 2004 indicates that claims 27-28 are rejected under 35 USC §102(e) as being anticipated by Winkler U.S. Patent No. 5,594,862 or in the alternative, rejected under 35 USC §103(a) as being obvious over Winkler in view of a text by Schneier (Applied Cryptography, 2nd ed., 1996). The office action also indicates that claims 1, 10, and 26 are rejected under 35 USC §103 as being unpatentable over Monroe et al. U.S Patent No. 5,293,388 in view of Davis U.S Patent No. 5825,879, Barnes et al. U.S Patent No. 4,172,213, Schneier, Poggio (CD ROM technical specification, April, 1988) and the applicant's admitted prior art (AAP). The '102 and '103 rejections are respectfully traversed.

Consider the example of a DVD drive coupled to a computer via a bus that is not secure. In this example, the DVD drive does not perform error correction (i.e., ECC-decoding) on all ECC blocks. Instead, certain ECC blocks are sent to the computer for ECC-decoding. The host computer can perform more flexible and more powerful error correction methods than the DVD drive.

The DVD drive could send unencrypted ECC blocks to the computer via the bus. Since the bus is not secure, however, the unencrypted ECC blocks would be vulnerable to theft and unauthorized copying.

The ECC blocks can't be encrypted by an encryption algorithm such as RSA, since integrity of the code words would be destroyed by the RSA encryption.

Thus, the example poses a problem: how to send ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying.

The office action cites six documents in the '102 and '103 rejections above. These cited documents, alone and in the aggregate, do not teach or suggest a solution to this problem.

Winkler discloses a RAID (Redundant Array of Independent Disks) type storage subsystem that includes a plurality of disk storage devices (such as magnetic disk drives) in electrical communication with a RAID disk storage device controller. Upon the receipt of a write or read command from a host computer, the RAID storage device controller writes blocks of data to or reads blocks of data from the disk storage devices. Depending upon the RAID implementation level, the blocks of data and the parity of the blocks of data are distributed among the disk storage devices. The controller performs XOR operations to generate a new parity value corresponding to new data being written from the host computer to a disk storage device in the storage subsystem.

For a description of parity data, see assignee's U.S. Patent No. 6,718,434. RAID is commonly used to provide protection against hard drive failure. Using RAID 1 (mirroring) or RAID 1/0 (striped mirroring), two copies of data are stored on different disks. For data storage devices having large numbers of disks, a more cost-effective method of fault protection is using partial redundancy such as parity. Using RAID 5 (striping with rotated parity), host data blocks are block-interleaved across the disks, and the disk on which the parity block is stored rotates in round-robin fashion for different stripes.

Poggio provides an introduction to CD technology. Poggio states that Cross Interleave Reed-Solomon Coding (CIRC) is employed for error correction. Page 3/8 also states that as each frame is read off a CD, it is it is decoded (first level error correction). Poggio also describes second level error correction, but states that second level error correction is performed in the CD drive (see the first paragraph of page 6/8)

Schneier describes XOR encryption. However, Schneier does not teach or suggest that XOR encryption can be used on ECC blocks. Moreover, Schneier suggests that XOR encryption is not a substitute for RSA encryption, since he states on page 14 that simple XOR encryption is "an embarrassment" and is "trivial to break."

Barnes, Monroe and Davis have already been addressed. However, their teachings will now be summarized.

Barnes et al. disclose a data encryption system that performs XOR encryption. However, Barnes et al are silent about ECC blocks.

As for Monroe et al., Figures 1-3 show a computer 10 including a host processor 80, a computer bus 20 that is connected to the computer 10, and a disk 30 that is connected to the bus 20 via an adapter 40. Figure 1 also shows a peripheral 50 (e.g., a backup tape drive) that is connected to the bus 20 via an adapter 60. The adapter 60 includes an ECC co-processor 65 and ECC RAM 66. The adapter sends compressed ECC data to the peripheral 50 (col. 1, lines 55-58). Monroe et al. do not teach or suggest encryption of ECC blocks.

In Davis, Figure 1 shows a computer including a processor 104 and disk control subsystem 108 that are connected to a bus 128. Figure 1 also shows a video subsystem 116 connected to the bus 128. The video subsystem 116 includes a secure video content processor (SVCP) 132 for converting incoming digital content into an analog signal (see col. 2, lines 54-58)

The SVCP 132 of Figure 1 corresponds to the SCVP 200 of Figure 2. The SCVP 200 includes decryption and decompression circuitry 228 that receives encrypted video content 212 from a video content source (e.g., CD ROM 220). According to Figure 5, encrypted digital video data is transmitted to the SVCP 200 (508), which decrypts the video data (512), processes the video data (514), re-encrypts the video data (516), and transmits the re-encrypted data to a memory unit.

Davis doesn't say much about the video source. The only passages appear to be located at col. 4, lines 27-31; and col. 6, lines 52-54. Neither of these passages mentions ECC blocks.

Thus, none of these cited documents address the problem of sending ECC blocks to a computer over an insecure bus without (1) destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. More generally, none of these cited documents even teach or suggest sending ECC blocks to a computer.

The applicant offers a solution to this problem. The applicant has found that a specific type of encryption -- XOR encryption -- offers the "unexpected advantage" of preserving the integrity of the ECC code words. ECC blocks can be XOR-encrypted in an optical drive, and sent to a host computer for error code correction. Because XOR encryption is used, the host can perform the error code correction without having to decrypt the block. Error-corrected data, still encrypted, could then be sent downstream to an authorized device (e.g., an authorized DVD decoder card) for decryption. Thus, the host computer could perform the error code correction, yet still not have access to the encrypted data.

Claims 27 and 28

Claim 27 recites a drive comprising a reader; and a controller programmed to perform a bitwise XOR of an encryption mask and a block of ECC-encoded data. A product of the bitwise XOR is an encrypted block. The controller is further programmed to output the encrypted ECC block.

Claim 28 recites a data controller comprising a processor for performing a bitwise XOR of an encryption mask and a block of ECC-encoded data, a product of the bitwise XOR being an encrypted block

Winkler does not teach or suggest encryption of any kind. Winkler does not teach or suggest hard drives that output ECC blocks. Winkler discusses the generation of RAID parity data. The parity data can be used with error-corrected data from good hard drives to recover data from a failed hard drive.

The office action states that Winkler's "parity [is] a technique for ECC encoding that is well known in the art." First, this statement is inaccurate, as indicated by U.S Patent No. 6,718,434. Second, the statement is irrelevant. Winkler's XOR operation is used to generate redundancy (parity) data. In contrast, claims 27 and 28 recite XOR encryption of blocks already containing redundancy data (ECC code words).

The office action cites col. 5, lines 21-33 of Winkler and states that parity data is a "partially encrypted block." However, Winkler does not support this statement. The cited passage simply indicates that generating new parity data (P_{new}) includes an XOR operation on new data (D_{new}), old data (D_{old}), and old parity data (P_{old})

The office action anticipated this argument, and stated "If Applicant contends that the result of the XOR controller is not an encrypted parity block, then it can be seen as an obvious development in light of the teachings of

Schneier. However, the office action does not explain how Schneier's teachings make claims 27-28 obvious. If this rejection is maintained, an explanation is respectfully requested. The explanation should consider Schneier's statement on page 14 that simple XOR encryption is "an embarrassment" and is "trivial to break."

Moreover, Winkler is not even analogous prior art. MPEP 2141 states "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." Winkler's generation of parity data is not relevant to encryption, nor is it pertinent to the problem of sending ECC blocks over a bus that is not secure.

For these reasons, claims 27 and 28 should be allowed over the combination of Winkler and Schneier.

Claims 1, 10 and 26

Claims 1, 10 and 26 recite a system including a drive for providing an encryption mask; and for performing a bitwise XOR of the encryption mask and a block of ECC-encoded data; the drive providing the encrypted block to the computer bus. This system allows an encrypted block can be sent to the host processor via the computer bus for error code correction.

Monroe et al., Monroe, Davis, Barnes, Schneier, AAP and Poggio, alone or in combination, do not teach or suggest sending ECC blocks to a computer. This point apparently is being missed in the office action. The office action argues that the cited documents show ECC correction being performed within a drive. Poggio, for example, states that first and second level error correction is performed on ECC data within a CD drive. Thus, the data leaving the drive does not consist of ECC blocks, but rather error-corrected data.

With this argument, however, the office action supports the applicant, not the rejection. Claims 1, 10 and 26 recite that ECC blocks (that is, blocks prior to error code correction) are outputted by a drive. These blocks are not error code-corrected. This allows error code correction to be performed by a host computer.

Moreover, Monroe, Davis, Barnes, Schneier, AAP and Poggio, alone or in combination, do not teach or suggest the encryption of ECC blocks. The office action acknowledges that Monroe et al. are silent about encryption of ECC blocks. Poggio is also silent about encryption of ECC data. Although Barnes discloses XOR encryption, Barnes is also silent about performing XOR encryption on ECC blocks.

Davis discloses an SCVP 200, which includes decryption and decompression circuitry 228 that receives encrypted video content 212 from a video content source (e.g., CD ROM 220). Davis does not state that video content consists of encrypted ECC blocks.

The office action observes that SVCP could be included in a DVD drive (at col. 7, lines 19-20). However, the observation is irrelevant, as it relates to the decryption of video content, not the encryption of ECC blocks.

Schneier is also silent about encryption of ECC blocks. Although Schneier discusses XOR encryption, he does not teach or suggest the desirability of using XOR encryption. To the contrary, Schneier actually gives a reason for NOT using XOR encryption. To reiterate, Schneier states on page 14 that simple XOR encryption is "an embarrassment" and is "trivial to break."

To summarize, none of these documents addresses the problem of how to send ECC blocks to a computer, without destroying the integrity of the ECC code words; and (2) not leaving the ECC blocks vulnerable to theft and unauthorized copying. Therefore, claims 1, 10 and 26 should be allowed over the documents made of record.

The office action also indicates that independent claims 1 and 26 are substantial duplicates; consequently, both would not be allowed. This rejection has been rendered moot by the amendment above to claim 1.

The office action also indicates that claims 1 and 26 are rejected under the judicially-created law of double patenting over claim 8 of U.S. Patent No. 6,252,961. If the claims are found to contain allowable subject matter, this rejection can be overcome with a terminal disclaimer.

The office action objects to the declaration for not including certain statements. A copy of the declaration is attached. It is the same declaration that was filed in parent application 09/053,972 (now, U.S. Patent No. 6,252,961). The attached copy has been annotated (see "A") to indicate that it does indeed contain these certain statements.

It is respectfully submitted that the present application is in condition for allowance. The examiner is encouraged to contact the undersigned to discuss any remaining issues.